工程与管理科学
Engineering and Management Science
第 7 卷◆第 11 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

# 区块链技术在网络安全中的应用与挑战

胡亚峰
中铁工程设计咨询集团有限公司　北京　100055

DOI：10.12238/ems.v7i11.16088

［摘　要］区块链技术具有机制透明可信、交易防篡改、隐私保护与系统可靠性高等特点，为网络安全提供了新的技术路径。本文分析了区块链技术在网络安全中的应用场景，介绍了区块链技术在计算机病毒库分布式存储系统中的典型应用，探讨了区块链技术面临的安全局限性、性能瓶颈制约与法律监管薄弱等挑战，提出了应对策略建议。

［关键词］区块链；网络安全；计算机病毒库

## 1 引言

近年来，从个人信息泄露到信息设施被攻击，从网络入侵到勒索软件威胁，网络安全事件频繁发生，攻击手段日益多样，传统的防护技术已不足以应对新型挑战[1]。区块链技术以块链式数据结构存储数据，以分布式节点共识算法更新数据，以密码学的方式保证数据传输与访问的安全性，以智能合约编程及操作数据，具有机制透明可信、交易防篡改、隐私保护与系统可靠性高等特点，可为网络安全提供了新的技术路径[2][3]。区块链技术在网络安全中的应用也面临诸多挑战，如安全局限性、性能瓶颈制约与法律监管薄弱等。本文将从应用场景、应用案例、面临挑战、应对策略建议与应用前景 5 个方面展开论述，为区块链技术在网络安全领域中的应用研究提供指导建议。

## 2 区块链技术在网络安全中的应用场景

### 2.1 数据信息安全

数据信息安全指通过技术手段保护数据信息的内容免受破坏、篡改或泄露，确保系统可靠运行与信息服务的连续性。区块链的防篡改、可追溯与高可靠性技术可以用于数据传输、验证与存储等环节。防篡改技术可用于数据传输环节，如基于共识算法记录数据交换活动，并将关键数据添加至区块链，则很难被修改或删除。可追溯技术可用于数据验证环节，基于区块链的日志机制，任意一次数据交换都有完整记录，可追查与其相关的全部历史数据交换。高可靠性技术可用于分布式数据存储系统的构建，每个节点独立维护账本并参与系统的更新，那么即使某些节点出现故障，整个系统依然正常运行；基于共识算法，系统可支持拜占庭容错，也即部分节点被攻克或被修改业务逻辑，整个系统依然可正常运行。

### 2.2 身份管理与认证

身份管理与认证指通过技术手段对计算机网络中的操作者身份真实性与有效性进行确认。传统的身份管理技术普遍采用中心化机制，各系统的身份数据单独存储于各自中心，数据泄露风险高、认证格式不统一且孤岛现象严重。针对以上弊端，区块链技术在身份管理机制、身份数据保护与身份认证方式上都有应用前景[2][4]。对于身份管理机制，基于点对点交易、分布式账本与共识机制，可构建去中心化的系统，形成多方共建共管的新型身份管理机制，从源头消除孤岛现象。对于身份数据保护，用户可将完整的个人身份数据存于本地，而只将部分身份数据或哈希值存于区块链上，那么即使单个节点被攻破，完整的用户数据也可得到有效保护。对于身份认证方式，既可将身份证明结果以加密方式发布于区块链上，认证机构根据用户授权来读取和验证身份信息；也可在智能合约中加入生物特征认证功能，以摆脱繁杂的密码或口令。

### 2.3 网络隐私保护

网络隐私保护指通过技术手段在网络环境中让自然人的活动及个人信息不被非法侵扰、收集或公开。区块链技术可用于个人活动保护与个人信息保护。对于个人活动保护，区块链中的用户以私匙作为唯一身份标识，可凭私匙参与各类交易，而系统不会记录私匙的持有者信息，进而实现了用户活动保护。因此基于区块链技术来构建网络活动交互机制，可有效防止个人活动被非法收集。对于个人信息保护，同态加密、零知识证明等区块链技术让数据以加密形式保存，可在不泄露数据内容的情况下证明数据的真实性，而任何不相关用户都无法从密文中获得有效信息，只有授权的交易用户才可在设定范围内访问和使用数据，这为用户隐私信息保护提供了技术保障。

## 3 计算机病毒库中的区块链技术应用案例

### 3.1 应用背景

计算机病毒指人为在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机正常使用并且能够自我复制的一组计算机指令或程序代码。计算机病毒库用于收集各类病毒样本，分析病毒特征信息并预测病毒发展趋势。当前病毒库虽对安全性有所考虑，但尚不够彻底，病毒样本存在被篡改的风险；存入管理功能较薄弱，自动化程度不高；大多是单点独立建设，存在瘫痪或数据丢失的风险，无法实现高可靠性。

文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

3.2 分布式存储节点结构

基于区块链的计算机病毒库分布式存储系统由接入互联网的存储节点构成，各存储节点间通过区块链实现同步与防篡改功能。分布式存储节点包括主控模块、智能合约模块、摘要提取模块、文件管理模块、磁盘阵列模块、病毒采集模块、病毒访问模块、状态显示模块及显示与鼠标键盘接口模块，其中智能合约模块与摘要提取模块构建于区块链上，如图 1 所示。

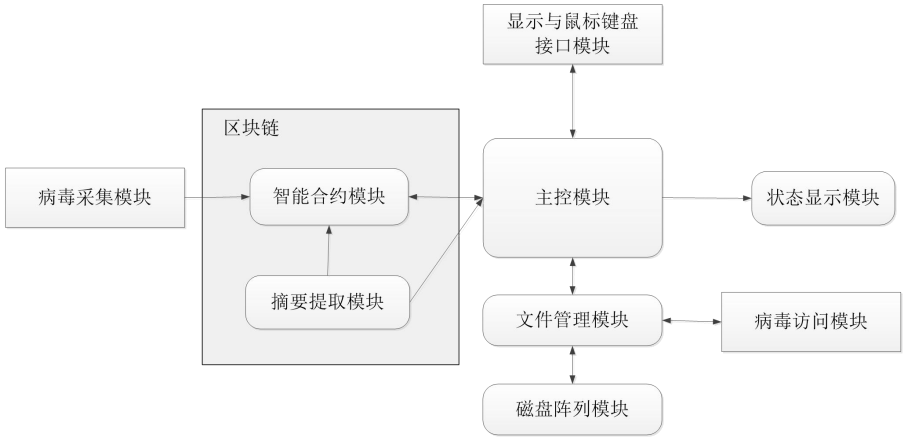


图 1　计算机病毒库分布式存储节点结构

主控模块负责整个系统工作流程控制，协调各个模块完成病毒样本的安全可靠存储。

智能合约模块在主控模块的控制下，利用事先存储在区块链上的合约，判别采集的病毒样本是否合格及病毒文件处理结果能否入链。对于采集的病毒样本，该模块判别病毒样本是否满足预先设定的合约条件，如果满足则按照合约规则将病毒样本交给主控模块，否则丢弃。对于病毒文件处理结果，该模块判别是否满足预先设置的合约条件，如果满足则按照合约规则将处理结果写入区块链。

摘要提取模块在主控模块与智能合约模块的控制下，通过安全散列算法提取病毒样本的摘要信息。安全散列算法以较短的信息作为原始文件的唯一性标志，这种标志与文件的每一个字节都相关，而且难以找到逆向规律。可采用 SHA256 安全散列算法，每个病毒文件提取 256 位哈希值。病毒摘要信息入链后，基于区块链的防篡改特性，通过校核摘要信息可保证病毒样本文件的完整性。

节点中的每个病毒存储内容包括病毒描述信息、对应区块哈希值与病毒文件。病毒描述信息包括存在形态、传播方式、对应操作系统及采集时间等，用于展示及检索。区块哈希值用于标识区块链中与该病毒关联的区块地址。病毒文件包含可执行病毒代码、被病毒感染的文档文件、嵌入病毒的数据文件与含病毒的源代码文件等。

3.3 区块结构

由于病毒样本格式多样且部分文件较大，本系统并不在区块链上直接存储原始病毒文件，而是存储操作信息、病毒文件索引与病毒文件摘要，以此实现各节点的病毒文件同步及防篡改功能。区块链的每个区块都是由块头与块体组成，块头含有连接上一区块的哈希值，块体用于存储病毒文件信息，如图 2 所示。存储操作信息由标识符、操作类型与操作发起方节点 ID 构成。病毒文件索引为固定长度的数值序列，根据该索引可从分布式存储系统中任一节点下载对应病毒文件。病毒文件摘要为固定长度的数值序列，作为原始文件的唯一性标志。对于病毒处理结果，首先将密码学签名的处理信息封装入区块，形成分布式数字帐本，然后经过数字签名确认，将该处理信息记录于下一待入链区块中，最后经过验证和共识算法选择，被选中的待入链区块作为新区块入链。

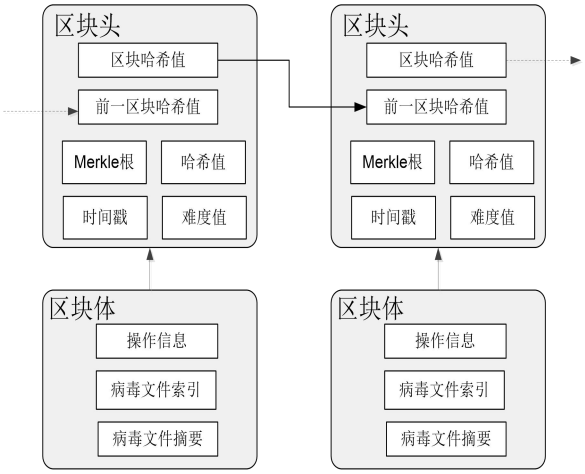


图 2　区块结构

3.4 分布式存储系统

计算机病毒库分布式存储系统由若干存储节点构成，各存储节点接入互联网，通过区块链实现病毒文件的同步与防篡改，如图 3 所示。每个节点由互不相同的 ID 标识，各节点的病毒库通过区块链保持同步。任意节点被移除或攻克，系统都不会受到影响。用户可通过 Web 浏览器或专用软件接入系统任一节点，查找所需的病毒信息，并下载相应病毒文件。

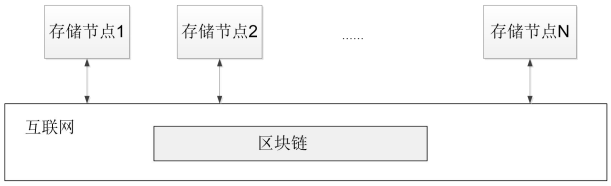


图 3　计算机病毒库分布式存储系统结构

## 4 区块链技术在网络安全中面临的挑战

### 4.1 安全局限性

区块链技术仍处于发展阶段，存在潜在的安全风险，影响其在网络安全领域的深度应用。首先，区块链中的智能合约容易出现漏洞与逻辑缺陷，而其一旦部署则很难修改，这可导致严重的网络安全风险。其次，区块链是开放的点对点账本系统，交易信息在一定程度上仍可被公开追溯和分析，这无法适用于网络隐私要求极高的应用场景。最后，单一的安全措施也是限制区块链应用的主要因素之一，私钥是证明所有权的唯一工具，而一旦私钥被泄露，则独立账户的安全性就无法得到保障。

### 4.2 性能瓶颈制约

区块链技术在处理能力、互操作性与灵活性方面存在性能瓶颈，影响其在网络安全领域的广泛应用。对于处理能力，区块链去中心化验证机制需要极高的计算成本，其代价是交易处理速度的下降，这在高处理速度、高延展性与高吞吐量的网络环境中无法广泛应用。对于互操作性，各区块链往往独立运行，数据和资产难以在不同链之间顺畅流通，而网络安全的集约化趋势对互联互通有着较高的要求，这也限制了区块链技术的应用场景。对于灵活性，区块链的核心在于共识机制，而该机制一旦形成就难以改变，导致了其在灵活性方面较弱，无法适用于复杂多变的网络安全场景。

### 4.3 法律监管薄弱

区块链作为一种全新的技术，能够让用户在公开和完全分布式的点对点系统中对所有权进行管理和转移，而交易双方身份信息隐匿，交易流向追踪困难，使得法律监管难度加大[5]。这种通过分布式共识参与管理所有权的方式颠覆了中心化管理的特质，相关的法律框架与监管机制则显得相对薄弱。网络安全一方面要求加强对隐私数据的保护，另一方面也要求安全事件的可审计性，需将违规行为纳入法律监管范围。因此，制定和完善区块链技术的法律法规是区块链技术在网络安全中合法应用的关键。

## 5 应对策略建议

### 5.1 加强关键技术攻关

针对区块链技术在网络安全领域面临的诸多挑战，加强关键技术攻关。如针对网络安全应用需求，从源头上优化共识机制，以既能大幅提高交易处理速度和网络效率，又能提高灵活性。又如针对网络安全互联互通需求，从密匙控制策略、区块结构与验证机制上进行改造，以增强其互操作性能。再如通过优化数据存储结构，采用新型数据库技术提升区块链的存储容量和访问效率。建议政府、企业与科研机构的共同努力，通过设立专项基金与开展产学研合作等方式，将科研成果快速转化为实际生产力。

### 5.2 发展融合技术

加强区块链技术与其它前沿技术的融合，为网络安全提供更全面更高效的支撑手段。如将区块链技术与物联网技术融合，可以实现传感器的身份认证和数据传输校验，进而扩展网络安全的应用范围。又如将区块链与大数据技术融合，可以实现海量数据的篡改鉴别，进而加深数据安全的防护深度。再如将区块链与人工智能技术融合，可实现多模态数据的智能分析，进而扩展网络安全的防护边界。

### 5.3 完善行业标准

针对区块链技术在网络安全中的应用，从法律政策、标准规范与技术工具等方面提早布局，推动合法有序发展。对于法律政策，建议政府及法律专家在网络安全相关法律中明确区块链技术的监管框架，保障该技术的合法应用和发展。对于标准规范，建议从应用场景、操作流程、功能指标、性能指标与接口协议等方面入手，制定统一的标准规范，促进不同区块链系统之间的互操作与兼容。对于技术工具，建议研制融合区块链技术的网络安全评估工具软件，为该技术在网络安全中的应用效果提供了一种系统、规范且可重复的测评方法。

## 6 结束语

区块链技术用于实现多方信任与高效协同，在数据信息安全、身份管理与认证、网络隐私保护等网络安全领域存在巨大的应用空间，如可构建计算机病毒库分布式存储系统。与此同时，该技术也面临安全局限性、性能瓶颈制约与法律监管薄弱等诸多挑战。通过加强关键技术攻关、发展融合技术与完善行业标准可有效应对这类挑战。随着区块链技术的日益完善，其将在网络安全领域迎来更广阔的应用前景。

## [参考文献]

[1]吴嘉诚,余晓. 网络安全风险评估方法研究综述[J]. 电子科技，2024，37（3）：10-17.

[2]杨旸，闾海荣等. 区块链隐私技术[M]. 北京：电子工业出版社，2023.

[3]华为区块链技术开发团队. 区块链技术及应用[M]. 北京：清华大学出版社，2019.

[4]朱金涛,魏银珍等. 基于区块链的去中心化动态身份认证系统[J]. 计算机应用与软件，2025，42（1）：334-337.

[5]高昊昱，曹春杰等. 区块链安全监管研究综述[J]. 通信学报，2025，46（4）：49-70.